

INFORMATION SERVER DEVICE EQUIPPED WITH CIPHERING PROCESSING FUNCTION**Publication number:** JP2002182560**Publication date:** 2002-06-26**Inventor:** SATO MIKIKO; OKAZAWA KOICHI**Applicant:** HITACHI LTD**Classification:****- International:** G06F21/20; G06F9/46; G06F15/00; G09C1/00; H04L9/08; G06F21/20; G06F9/46; G06F15/00; G09C1/00; H04L9/08; (IPC1-7): G09C1/00; G06F9/46; G06F15/00; H04L9/08**- European:****Application number:** JP20000383117 20001212**Priority number(s):** JP20000383117 20001212**Report a data error here****Abstract of JP2002182560**

PROBLEM TO BE SOLVED: To provide a means for preventing a secret key from leaking and a means for reallocating computer resources of an information server device according to the busyness of processing for cipher communication and non-cipher communication while evading a decrease in the response speed of the information server device due to cipher processing. **SOLUTION:** A normal OS which logically divides the computer resources of the information server device and administers the transmission and reception of information and a secure OS which administers a function of deciphering a ciphertext ciphered with an open key at a request from the normal OS are placed in operation. Further, the device is provided with a means which measures information on the CPU use rates of the secure OS and normal OS and information on the memory use rates, informs a system administrator of the computer resource use state of the information server device when a set threshold is exceeded, and allows the system administrator having been informed to reallocate the computer resources of the information server device.

Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-182560

(P2002-182560A)

(43) 公開日 平成14年6月28日 (2002.6.28)

(51) Int.Cl.⁷

識別記号

F I

テーマコード* (参考)

G 0 9 C 1/00

6 2 0

G 0 9 C 1/00

6 2 0 Z 5 B 0 8 5

G 0 6 F 9/46

3 5 0

G 0 6 F 9/46

3 5 0 5 B 0 9 8

15/00

3 3 0

15/00

3 3 0 A 5 J 1 0 4

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

6 0 1 E

審査請求 未請求 請求項の数21 O L (全 18 頁)

(21) 出願番号

特願2000-383117(P2000-383117)

(22) 出願日

平成12年12月12日 (2000. 12. 12)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 佐藤 未未子

神奈川県海老名市下今泉810番地 株式会社日立製作所インターネットプラットフォーム事業部内

(72) 発明者 岡澤 宏一

神奈川県海老名市下今泉810番地 株式会社日立製作所インターネットプラットフォーム事業部内

(74) 代理人 100075098

弁理士 作田 康夫

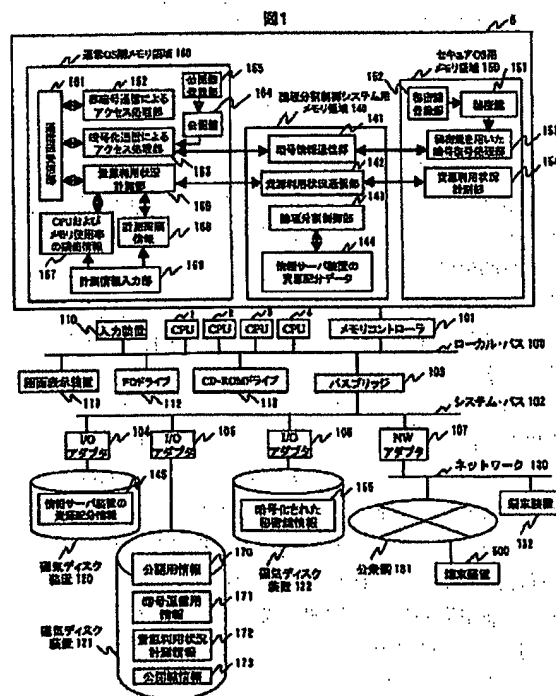
最終頁に続く

(54) 【発明の名称】 暗号処理機能を備えた情報サーバ装置

(57) 【要約】

【課題】 暗号処理による情報サーバ装置の反応速度低下を回避しつつ、秘密鍵の漏洩を防ぐ手段、および、情報サーバ装置の計算機資源を、暗号通信、非暗号通信の処理の忙しさに応じて再配分するための手段を提供することである。

【解決手段】 情報サーバ装置の計算機資源を論理的に分割し、情報の送受信を司る通常OSと、通常OSからの依頼に基づき、公開鍵で暗号化された暗号文を復号処理する機能を司るセキュアOSとを稼働させる。また、セキュアOSおよび通常OSのCPU使用率の情報と、メモリ使用率の情報とを計測し、設定した閾値を超えた場合に、システム管理者に情報サーバ装置の計算機資源使用状況を通知し、前記通知を受けたシステム管理者が情報サーバ装置の計算機資源を再配分する手段を設ける。



【特許請求の範囲】

【請求項 1】ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う、情報サーバ装置における公開鍵暗号処理の負荷分散方法において、前記端末装置に配布される公開鍵に対応する秘密鍵を、前記情報サーバ装置で実行される暗号処理プログラムの専有するメモリ領域に保持するステップと、前記端末装置により前記公開鍵を用いて暗号化され、前記情報サーバ装置にネットワークを介して送信された情報を受信した前記情報サーバ装置で実行される他のプログラムから、前記暗号化された情報とその復号化依頼を前記暗号処理プログラムにより受信するステップと、前記公開鍵を用いて暗号化された情報を、前記秘密鍵を用いて前記暗号処理プログラムにより復号化するステップと、前記暗号処理プログラムから前記復号化を依頼した前記他のプログラムへ、前記復号化した情報を返信するステップと、を有することを特徴とする公開鍵暗号処理方法。

【請求項 2】前記公開鍵で暗号化される情報が、前記端末装置と前記情報サーバ装置の間の共通鍵暗号方式による通信で用いられる共通鍵であることを特徴とする請求項 1 に記載の公開鍵暗号処理方法。

【請求項 3】前記暗号処理プログラムは、前記情報サーバ装置上で実行される前記他のプログラムとのみ通信を行うことを特徴とする請求項 1 に記載の公開鍵暗号処理方法。

【請求項 4】前記暗号処理プログラム及び前記他のプログラムが使用する CPU とメモリの使用率をそれぞれ計測するステップと、前記暗号処理プログラムと前記他のプログラムのそれぞれに対しあらかじめ決定された前記 CPU と前記メモリの使用率の閾値を保持するステップと、前記暗号処理プログラムと前記他のプログラムのそれぞれについて、計測された前記使用率と前記閾値を比較することで前記使用率が前記閾値を越えたかを監視するステップと、前記使用率が前記閾値を越えていた場合に、前記暗号処理プログラムと前記他のプログラムが使用する前記 CPU と前記メモリの使用率の再配分を行うステップと、を有することを特徴とする、請求項 1 に記載の公開鍵暗号処理方法。

【請求項 5】ネットワーク上の端末装置が公開鍵で暗号化した情報をネットワークを介して受け取り、前記公開鍵に対応する秘密鍵を用いて複合化する情報サーバ装置において、前記端末装置から送信された前記暗号化した情報を受信した他のプログラムから、前記暗号化した情報およびその復号化依頼を受け取り、前記公開鍵に対応する秘密鍵を前記他のプログラムの読み書きが許可されていないメモリ領域に保持し、前記復号化依頼を受信して前記暗号化された情報の復号化を前記秘密鍵を用いて行い、前記復号化した情報を送信元の前記他のプログラムに返信する暗号処理プログラムが稼動することを特徴とする情報サーバ装置。

【請求項 6】前記公開鍵で暗号化される情報が、ネットワーク上の端末装置と前記情報サーバ装置の間で行われる共通鍵暗号方式の通信に用いる共通鍵であることを特徴とする請求項 5 に記載の情報サーバ装置。

【請求項 7】前記暗号処理プログラムが情報の送受信を行う対象は、前記他のプログラムのみであることを特徴とする請求項 5 に記載の情報サーバ装置。

【請求項 8】前記暗号処理プログラムは、ネットワーク上に情報を送出しネットワーク上の情報を受信するネットワーク通信機能を持たないことを特徴とする請求項 5 に記載の情報サーバ装置。

【請求項 9】前記情報サーバ装置上で稼動する各プログラムが、前記各プログラムが使用する CPU 及びメモリの資源使用率を所定の時間毎に計測する手段と、計測された前記資源使用率の情報を保持する手段と、計測された前記資源使用率を前記情報サーバ装置の出力装置に出力する手段と、を有することを特徴とする請求項 5 に記載の情報サーバ装置。

【請求項 10】計測される前記資源使用率に対する閾値を入力する手段と、入力された前記閾値を保持する手段と、前記 CPU 及び前記メモリの資源使用率を設定する手段と、を有することを特徴とする請求項 9 に記載の情報サーバ装置。

【請求項 11】計測された前記資源使用率と前記閾値を比較し、計測された前記資源使用率が前記閾値を越えたかを監視する手段と、計測された前記資源使用率が前記閾値を越えた場合に、計測された前記資源使用率及び、前記閾値を越えた事を前記出力装置に出力し、各プログラムに対する計算機資源の再配分を行う手段を有することを特徴とする請求項 10 に記載の情報サーバ装置。

【請求項 12】論理分割制御システムにより、前記情報サーバ装置が有する計算機資源のうち少なくとも CPU 及びメモリを各プログラムに対し配分する手段及びそのための入力装置と、各プログラムに対する前記計算機資源の分配の状況を出力する手段及びそのための出力装置を有することを特徴とする請求項 5 に記載の情報サーバ装置。

【請求項 13】前記出力装置に、論理分割制御システムにより分割された前記計算機資源の各論理分割単位ごとに前記論理分割単位を識別するための情報、前記論理分割単位の名称、少なくとも前記論理分割単位が使用する前記 CPU 使用率及び前記論理分割単位が使用する前記メモリの容量、前記論理分割単位の OS 起動用のデバイスを識別するための情報、前記論理分割単位が使用する割り込み要求番号、前記論理分割単位の種別ごとの、割り当てられた前記メモリの容量、未使用の前記メモリの容量、を出力する第一の出力手段と、前記計算機資源の再配分を行うために前記入力装置から入力された、前記論理分割単位の名称、少なくとも前記論理分割単位にこれから使用させる前記 CPU の使用率及び前記論理分割

単位にこれから使用させる前記メモリ容量、を前記出力装置に出力する第二の出力手段と、を有することを特徴とする請求項12に記載の情報サーバ装置。

【請求項14】ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う情報サーバ装置で実行される少なくとも一つのプログラムを記録したプログラム記録媒体において、前記少なくとも一つのプログラムが、前記端末装置に配布される公開鍵に対応する秘密鍵を、前記情報サーバ装置で実行される前記少なくとも一つのプログラムにより専有されるメモリ領域に保持するステップと、前記端末装置から前記情報サーバ装置へ送信された前記公開鍵で暗号化された情報を、前記情報サーバ装置上で実行される他のプログラムを介して受け取るステップと、前記秘密鍵を用いて前記他のプログラムから受け取った情報の復号化を行うステップと、前記復号化された情報を前記他のプログラムに返信するステップと、を有するプログラムであることを特徴とするプログラム記録媒体。

【請求項15】少なくとも論理的に分割されたCPU及びメモリ領域と、ネットワークに対し情報の送受信を行うネットワーク接続装置を場合により割り当てられ、その上で少なくとも一つ以上のプログラムが実行される仮想計算機を、少なくとも二台以上有する情報サーバ装置において、一つの前記仮想計算機上で実行される暗号処理プログラムが、前記暗号処理プログラムが実行される前記仮想計算機とは異なる他の、前記ネットワーク接続装置を割り当てられた前記仮想計算機で実行されるプログラムにより受信された、ネットワーク上の端末装置により公開鍵を用いて暗号化された情報を、前記公開鍵に対応する秘密鍵を用いて復号化することを特徴とする情報サーバ装置。

【請求項16】前記秘密鍵は前記暗号処理プログラムが専有するメモリ領域に保持されることを特徴とする請求項15に記載の情報サーバ装置。

【請求項17】前記仮想計算機に割り当てられた前記CPU又は前記メモリ領域もしくはその両方について前記仮想計算機ごとに使用状況を計測し、前記使用状況に対するあらかじめ設定された閾値と比較し、前記閾値を超えた前記仮想計算機の前記CPU又は前記メモリ領域の使用量を増加せしめる手段を有することを特徴とする請求項15に記載の情報サーバ装置。

【請求項18】ネットワーク上の端末装置が公開鍵で暗号化した情報をネットワークを介して受け取り、前記公開鍵に対応する秘密鍵を用いて複合化する情報サーバ装置において、前記情報サーバ装置の少なくともCPU及びメモリ領域が論理的に分割され、分割された前記CPU及びメモリ領域ごとに、一つ以上のプログラムを実行する仮想計算機が少なくとも二つ以上稼動する前記情報サーバ装置であって、前記仮想計算機のうちの少なくとも一つの仮想計算機が、前記端末装置から送信された前

記暗号化した情報を受信した、前記少なくとも一つの仮想計算機とは異なる他の仮想計算機が実行する他のプログラムから、前記暗号化した情報およびその復号化依頼を受け取り、前記公開鍵に対応する秘密鍵を専有するメモリ領域に保持し、前記復号化依頼を受信して前記暗号化された情報の復号化を前記秘密鍵を用いて行い、前記復号化した情報を送信元の前記他のプログラムに返信する暗号処理プログラムを実行することを特徴とする情報サーバ装置。

10 【請求項19】前記暗号処理プログラムが稼動する仮想計算機は、ネットワークに対し情報の送受信を行うネットワーク通信機能を持たないことを特徴とする請求項18に記載の情報サーバ装置。

【請求項20】前記仮想計算機に割り当てられた論理的な前記CPU及び前記メモリ領域の使用状況を、前記仮想計算機ごとに計測し、計測した前記使用状況とあらかじめ設定された前記使用状況を比較し、計測した前記使用状況があらかじめ設定された前記使用状況を超えている場合は、前記仮想計算機が使用する前記CPUもしくは前記メモリ領域又はその両方の使用量を増加させることを特徴とする請求項18に記載の情報サーバ装置。

【請求項21】前記仮想計算機間の通信は、前記少なくとも一つの仮想計算機が専有する前記メモリ領域に通信を行うデータを格納し、前記他の仮想計算機が、前記第1の仮想計算機が専有する前記メモリ領域から前記データを取得することで行われることを特徴とする請求項18に記載の情報サーバ装置。

【発明の詳細な説明】

【0001】

30 【発明の属する技術分野】本発明は、ネットワークに接続された端末装置と情報サーバ装置間で公開鍵暗号方式を用いて機密性の高い情報を通信する際に、情報サーバ装置で行う公開鍵暗号方式の復号化処理の負荷を、情報サーバ装置で備える計算機資源を有効に活用することで軽減する方法に関する発明である。

【0002】

【従来の技術】インターネットに接続された、一般的なWebクライアントであるパーソナル・コンピュータやATM (Automatic Teller Machine)、カードリーダー等の個人認識を行うための入力装置を場合により持つコンピュータ等の端末装置は、Webサーバに代表される、インターネットに接続された情報サーバ装置と通信し、所望の情報の取得や送付を行う。

【0003】今日のインターネットでは、サーバに掲載する情報の取得という目的以外に、インターネットを利用した商品注文や、銀行取引、株の売買といったことが可能となっている。このような流通を行ったり金融情報を掲載しているサイトに対して、端末装置を操作するユーザが、ユーザの個人情報、クレジットカード番号、暗

証番号といった他人には知られたくない情報を、インターネットを経由して送信する必要がある。従来、他人に知られても良い一般的な情報に関しては、暗号化されていない平文が送受信されるが、前述したような機密情報に関しては、安全な送受信を行うために「SSL (Secure Sockets Layer)」という暗号通信を使うのが一般的である。

【0004】SSLでは、現在普及している公開鍵暗号方式が用いられる。公開鍵暗号方式とは、秘密鍵と公開鍵と呼ばれる2つの種類の鍵を用いて、一方の鍵で暗号化した情報を、他方の鍵で復号化するという暗号方式である。公開鍵暗号方式で使われる鍵は、一方向関数と呼ばれる数学的な計算手順で決められるものなので、片方の鍵（公開鍵）が分かっても、もう片方の鍵（秘密鍵）を解読することはほぼ不可能としている。

【0005】また、公開鍵暗号方式は、従来の共通鍵暗号方式（お互いに共通の暗号鍵を持ち、暗号情報の送受信を行うもの）に比べ、暗号処理の計算量が増大することが知られている。一方で、公開鍵暗号方式は、従来の共通鍵暗号方式に比べて、公開鍵は秘匿する必要がないので鍵の配布が容易であり、インターネットでの暗号通信に適した方式である。またSSLは、前記各々の暗号方式の利点を活かした暗号通信手順となっている。すなわち、実際に端末装置と情報サーバ間で交換する機密情報の送受信には、計算処理量が軽い共通鍵暗号方式を用い、その共通鍵暗号方式に用いる共通鍵の送受信に公開鍵暗号方式を用いる、という通信方式となっている。

【0006】尚、SSLについては、日経インターネットテクノロジー特別付録「EC時代のWebシステム高速化」（日経BP社、2000年12月号、p33～p35）に詳しい。

【0007】しかし、この公開鍵暗号方式を処理する情報サーバ装置のCPU (Central Processing Unit) は、公開鍵暗号方式の復号化処理に多くの時間を必要とし、また復号化処理を速く行うには多くのメモリ容量が必要であり、情報サーバ装置の負荷が増大することが知られている。このことにより、例えば、SSL通信機能を持つ情報サーバ装置に対し、SSL通信を行う複数の端末装置から同時に多数のアクセス要求が発生した場合、情報サーバ装置から端末装置への応答速度が極端に低下してしまう、という問題が発生する。

【0008】現状では、以下の方法で、情報サーバ装置への公開鍵暗号処理による負荷を軽減している。

【0009】(1) サーバを複数台設ける方法
非暗号通信によるアクセスを受け付ける情報サーバ装置と、暗号通信によるアクセスを受け付ける情報サーバ装置とを別々に設ける。これらの情報サーバ装置は、端末装置を利用するユーザからはどちらの情報サーバ装置とも通信可能となるよう、ネットワークに接続されてい

る。

【0010】(2) アクセラレータ装置を導入する方法
暗号処理専用のアクセラレータ装置を情報サーバ装置に接続し、暗号処理をアクセラレータ装置で行い、本来の情報サーバ装置の処理、すなわち、端末装置との情報送受信、受信情報の処理、送信情報の作成等にCPUを使用する。

【0011】しかしながら、これらの方法にはそれぞれ問題点がある。

10 【0012】(1) サーバを複数設ける方法の問題点
公開鍵暗号方式を処理する情報サーバ装置では、一般的に、秘密鍵の情報を暗号化して、磁気ディスク等の記憶装置内に機密保管しておく。復号処理に秘密鍵を用いる際に、特定のパスフェーズを入力しなければ、秘密鍵を使用するアプリケーションから読み取れない仕組みがほどこされている。そして、パスフェーズが入力されれば、情報サーバ装置のメモリ内に秘密鍵の情報がロードされ、暗号の復号処理に用いられる。

20 【0013】通常のOS (オペレーティングシステム) では、障害発生時に、メモリに保持されている全ての情報を、磁気ディスク装置へ格納する手段がとられる（メモリダンプと呼ばれる）。これは、サーバ装置を、障害発生前の状態に復帰させたり、または、障害発生の原因究明に利用するために行われる。

【0014】もし、メモリ上に秘密鍵の情報が保持されている時に障害が発生し（あるいは、故意に障害を発生させられ）、メモリダンプが生成されれば、秘密鍵の情報は暗号化されない状態で磁気ディスク装置へ格納される可能性がある。

30 【0015】そして、このような情報サーバ装置がネットワークに接続され、遠隔より障害復旧等の作業をする場合、ネットワークに接続された他の端末装置から、磁気ディスク装置やメモリ内の情報を読み取られる可能性がないとは言えない。

【0016】(2) アクセラレータ装置を導入する方法の問題点

アクセラレータ装置では、秘密鍵をアクセラレータ内の不揮発性メモリ内に登録し厳重に保管する機能を設けており、情報サーバ装置のメモリ上、および、情報サーバ装置に付属する磁気ディスク装置上には秘密鍵を置かずに、暗号処理する仕組みとなっている。そのため、秘密鍵の漏洩をほぼ完全に防ぐことが可能である。

40 【0017】しかし、そういった機能をもつアクセラレータ装置1台の価格は、一般の情報サーバ装置1台分の価格にほぼ相当するものもあり、大変高価である。この大きな投資をしたアクセラレータ装置は暗号処理専用機器なので、暗号処理が頻繁に行われない時間が存在しても、その間にアクセラレータ装置内に備え付けられているCPUやメモリなどの資源を他の目的に使用することはできない。

【0018】以上の問題点の他に、以下の問題点も残されている。情報サーバ装置の暗号通信と非暗号通信がどの位の割合で発生するものかは、情報サーバ装置に掲載する情報（すなわち、一般に公開する情報）、あるいは、時刻によっても変動するものであり、一概に予測できるものではない。

【0019】サーバを複数設ける方法、あるいは、アクセラレータ装置を導入する方法の場合、ある程度、暗号および非暗号通信の変動を予想して情報サーバ装置のシステム構成を考える必要がある。そして、一度決定した

システム構成を、安易に変更することはできない。

【0020】

【発明が解決しようとする課題】このように従来の技術では、公開鍵暗号方式による通信を行う情報サーバ装置において、秘密鍵を用いた復号化処理の負荷が高くなった場合に、その他の処理を行う負荷の小さなCPUや使用されていないメモリ等の計算機資源を、復号化処理のために使用することが容易では無かった。また復号化処理専用の処理装置を用意しても、その装置のCPUやメモリを他の用途に使用することができず、計算機資源の有効利用をすることができなかった。

【0021】また従来の技術では、情報サーバ装置が保持する秘密鍵の秘匿性が低下する場合が存在する。

【0022】

【課題を解決するための手段】そこで上記課題を解決するために本発明では、以下に説明する公開鍵暗号処理の負荷分散方法、及びこの方法を用いた情報サーバ装置を提供する。

【0023】本発明の、ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う情報サーバ装置上では、稼動する複数のプログラムのうちの一つである暗号処理プログラムが秘密鍵の保持及びこの秘密鍵を用いた情報の復号化を一手に処理するよう設定される。情報サーバ装置と端末装置間における、ネットワークを介した情報の送受信処理は、暗号処理プログラム以外の、ネットワーク接続装置を制御する他のプログラムが行う。他のプログラムが受信した情報が公開鍵で暗号化された情報であった場合は、暗号処理プログラムに受信した情報の復号化を依頼する。そして暗号処理プログラムは情報を復号化すると、復号化依頼をした他のプログラムに復号化した情報を返送し、その後のこの情報に関する処理は他のプログラムにて行われる。

【0024】復号化処理を行う暗号処理プログラムがネットワーク通信機能を持たない、つまりネットワーク接続装置を用いたネットワーク上の端末装置との通信を直接に行わないよう設定されていれば、ネットワーク上の端末装置やその他機器は、ネットワーク接続装置を制御する他のプログラムを介して暗号処理プログラムにアクセスすることとなる。つまり、ネットワーク上の第三者が暗号処理プログラムに直接アクセスすることはでき

ず、暗号処理プログラムが秘密鍵を専有するため秘密鍵の機密性は高まり、秘密鍵の情報漏洩を防ぐことができる。さらに障害発生時に、暗号処理プログラムがメモリダンプ情報を生成しないように設定されていれば、秘密鍵の情報漏洩の防止効果をさらに高めることができる。

【0025】また、秘密鍵を用いた復号化処理を行う暗号処理プログラムと、その他のプログラムについて、各々のプログラムが用いるCPUやメモリ等の計算機資源の使用率等の使用状況を所定の時間毎、つまり装置の管理者等に設定された時間間隔ごとに計測し、この計測された使用状況が所定の値に達した場合に計算機資源の再配分を行うことで、暗号処理とその他処理の負荷の変動に応じた計算機資源の有効活用を行うことができる。

【0026】

【発明の実施の形態】本発明の一実施形態を、図面を参照して以下に説明する。図1に、本実施形態の情報サーバ装置の構成図を示す。情報サーバ装置にはローカルバス100を設け、当該情報サーバの各種処理を実行するCPU (Central Processing Unit) 1~4と、種々の情報を格納するメモリ5を接続するためのメモリコントローラ101と、情報サーバ装置に各種情報を入力するキーボードやマウス等の入力装置110と、出力装置として情報サーバ装置の各種情報を表示するモニタ等の画面表示装置111と、FD (Floppy Disk) に対して情報を読み書きするFDドライブ112と、CD-ROM (Compact Disk ROM) に対して情報を読み書きするCD-ROMドライブ113と、各種入出力装置を接続するためのシステムバス102とローカルバス100とを接続し制御するバスブリッジ103を備える。システムバス102には、前記バスブリッジ103の他に、磁気ディスク装置等の外部記憶装置120~122を接続するためのI/Oアダプタ104~106と、LAN (Local Area Network) 等のネットワーク130を接続するためのネットワーク接続装置である、ネットワーク用アダプタ107を備える。これら計算機資源は後述する論理分割制御システムにより分割され、それらCPUやメモリ領域、その他記憶装置等の一部ずつが論理分割単位としてまとめられ、この論理分割単位の計算機資源を使用して仮想計算機が稼動し、その上でOSが実行される。この後の説明に用いる通常OSとセキュアOSは、それぞれ異なる仮想計算機上で実行されるOSである。

【0027】本実施形態では、CPUの数を4つとしているが、情報サーバ装置のCPUがこれ以下であったり、もしくはこれ以上のCPUを有していても良い。また、出力装置としてモニタ等の画面表示装置を例示したが、この他にプリンタ等の印刷機械が接続されて、情報サーバ装置の各種情報が紙面に印刷されても良い。また、携帯性に優れた情報記録媒体を用いるための装置と

して、前述のFDドライブやCD-ROMドライブの他にDVD-RAM (Digital Versatile Disk RAM) ドライブやMO (Magnetic Optical) ドライブのような、その他の携帯性に優れた情報記録媒体用の装置が接続されていてもよい。また、図1において、ネットワーク用アダプタを一つのみ図示しているが、複数のネットワーク用アダプタがシステム・バスに接続されていてもよい。

【0028】ネットワーク130は、例えば、WAN (Wide Area Network) 等の公衆網131に接続されており、情報サーバ装置は、公衆網131およびネットワーク130を経由して、公衆網131に接続された任意の端末装置500と通信する。また、ネットワーク130には、本情報サーバ装置からの資源再配分要求を受信するための端末装置132が接続されている。

【0029】システム管理者は、入力装置110や画面表示装置111を用いて、情報サーバ装置の資源配分を行うことができるが、端末装置132を用いて情報サーバ装置の資源配分の決定等を行うこともでき、この場合は資源配分に必要な情報が出力される出力装置は情報端末132のモニタ等となる。以下、システム管理者は端末装置132を介して情報サーバ装置からの資源配分要求を受け、実際の作業は場所を移動して入力装置110と画面表示装置111を用いて行うこととして実施例を示す。

【0030】メモリ5上には、情報サーバ装置の計算機資源を論理分割するシステム用のメモリ領域140と、暗号処理を司るセキュアOS用メモリ領域150と、端末装置500からのアクセス要求に応えたり、情報サーバ装置の資源利用状況を計測する処理を司る通常OS用メモリ領域160とを備える。本実施例では、秘密鍵を保持しそれを用いた情報の復号処理を行う暗号処理プログラムがセキュアOSに、他のプログラムが通常OSに相当する。

【0031】本発明における情報サーバ装置の計算機資源を論理的に分割し、各計算機資源上でOSを実行させ、それらOS間の通信を仲介するシステム・プログラムである論理分割制御システムが使用する。論理分割制御システム用メモリ領域140は、通常OSとセキュアOS間の暗号情報の通信を司る暗号情報通信部141と、通常OSとセキュアOS間で資源利用状況に関する情報の通信を司る資源利用状況通信部142と、情報サーバ装置の計算機資源を論理的に分割する処理を司る論理分割制御部143と、論理分割制御部143から参照する現状配分されている計算機資源の配分情報を納めるメモリ領域144とを有する。

【0032】通常OSとセキュアOSは、論理分割制御システムが提供する暗号情報通信部141や資源利用状況通信部142を介して通信を行う。この仮想計算機間

の通信は様々な方法で実行することができ、例えば共有ディスクを用意して各仮想計算機がそれに対しアクセスを行う方法や、物理的に通信インタフェースを設けこのインタフェースを介して通信を行う方法がある。

【0033】又、通常OS、セキュアOSがそれぞれ有するメモリ領域を介した通信も考えられる。このメモリ領域を介した通信を行うには、情報サーバ装置を起動する時に、通常OS用メモリ領域160に仮想計算機間通信用のメモリ領域を確保し、同じくセキュアOS用メモリ領域にも仮想計算機間通信用のメモリ領域を確保する。通常OSからセキュアOSにデータを送信する場合は、まず通常OSがその仮想計算機間通信用のメモリ領域にデータを格納する。そして通常OSは、データが格納されているメモリ領域の先頭アドレスやデータのサイズ、通信相手（この場合はセキュアOS）等を目的に応じて論理分割制御システムの暗号情報通信部141もしくは資源利用状況通知部142に通知する。通知を受けた論理分割制御システムの暗号情報通信部141や資源利用状況通知部142といったOS間通信用プログラムは、通信相手をセキュアOSと識別したら、このセキュアOSが稼動する仮想計算機に対し割り込み要求を通知する。この割り込み要求に対する応答を受けたOS間通信用プログラムは、先に通常OSから受信した、データが格納された先頭アドレスやデータのサイズ等の情報をセキュアOSに通知し、そのメモリ領域からセキュアOSのメモリ領域にデータを格納する処理を行うよう要求する。セキュアOSはこの要求を受け、そのデータを格納するため確保したセキュアOS用メモリ領域の一部にデータを格納する。

【0034】セキュアOSから通常OSへデータを送信する場合も同様であるが、セキュリティを高めるために通常OSがセキュアOS用メモリ領域150に一切アクセス出来ないようにするのであれば、論理分割制御システム用メモリ領域140の一部にセキュアOSが送信を要求するデータを一度格納し、そのデータを通常OSが通常OS用メモリ領域に格納するようにすれば良い。もしくは、通常OS用メモリ領域160にセキュアOSが直接データを格納しても良い。このように、メモリ領域を介して各仮想計算機上のOSが通信を行う場合は、論理分割制御システム上のOS間通信用プログラムは、あるOSからのメモリ領域へのアクセス要求を通信相手のOSに通知するという処理を行う。

【0035】論理分割制御部143は、入力装置110からの入力を受け付け、前記資源配分情報144を更新したり、更新した情報に基づいて、本情報サーバ装置上で稼動する仮想計算機が使用する計算機資源を配分し直す機能を備える。また、前記論理分割制御部143は、前記資源配分情報144が更新された際に、更新された資源配分情報144を磁気ディスク装置120内の資源配分情報145へ格納する機能を持つ。また、本情報サ

サーバ装置に電源を投入した時に、前記資源配分情報145の内容の一部を資源配分情報144へコピーし、コピーした資源配分情報144を参照しながら、本情報サーバ装置を稼動する機能を備える。

【0036】セキュアOS用メモリ領域150はセキュアOSが専有するメモリ領域であり、公開鍵暗号の復号化に用いる秘密鍵を入力装置110から入力してメモリ領域151に格納し、さらに秘密鍵を暗号化して磁気ディスク装置122内の秘密鍵情報155へ格納したり、セキュアOS起動時に磁気ディスク装置122から暗号化された前記秘密鍵情報155を読み出し、入力装置110から入力するパスフレーズで復号化し、前記秘密鍵を納めるメモリ領域151へ格納する機能を備えた秘密鍵登録部152と、秘密鍵を用いた暗号処理を司る暗号復号処理部153と、セキュアOSの資源利用状況を計測する資源利用状況計測部154とを備える。

【0037】通常OS用メモリ領域160は通常OSが用いるメモリ領域であり、ネットワーク130を介して端末装置500と通信する通信送受信部161と、磁気ディスク装置121に保持している公開鍵情報170を非暗号通信により端末装置へ提供する処理を司るアクセス処理部162と、磁気ディスク装置121に保持している暗号通信情報171を暗号化通信により端末装置へ提供する処理を司るアクセス処理部163と、アクセス処理部163の暗号通信に用いる公開鍵情報を、入力装置110から入力し公開鍵のメモリ領域164に登録し、さらに磁気ディスク装置121内の公開鍵情報173へ格納したり、通常OS起動時に前記公開鍵情報173を読み出し公開鍵のメモリ領域164へ格納する機能を備えた公開鍵登録部165とを備える。

【0038】また、通常OS用メモリ領域160では、通常OSの処理の忙しさを計測する資源利用状況計測部166と、前記資源利用状況計測部166から参照されるCPUおよびメモリ使用率の閾値情報167と、計測間隔情報168と、前記閾値情報167と計測間隔情報168を入力装置110から入力し登録する計測情報入力部169を備える。また、セキュアOS用メモリ領域150には、セキュアOSの処理の忙しさを計測する資源利用状況計測部154が存在する。

【0039】閾値情報と計測間隔情報については、磁気ディスクにこれら情報を格納する領域を設け、通常OSもしくはセキュアOS起動時に磁気ディスク装置から読み出され、それぞれが閾値情報167と計測間隔情報168に格納され、またこれら処理を行う閾値・計測間隔情報登録部が通常OS用メモリ領域160に存在してもよい。

【0040】前記CPU使用率とは、割り当てられたCPUの何パーセント(%)を使用してプログラムを実行しているかを示す情報である。また、前記メモリ使用率とは、割り当てられたメモリ容量の何パーセント(%)

を使用してプログラムを実行しているかを示す情報である。また、前記閾値情報とは、通常OSおよびセキュアOSのCPU資源の使用率、および、メモリ資源の使用率の使用限界、すなわち、処理をこなすために必要な計算機資源が不足したことを示す閾値もしくは境界値である。また、計測間隔情報とは、前記CPU使用率とメモリ使用率を計測する間隔を示す情報である。システム管理者は、閾値情報および計測間隔情報を、情報サーバ装置の稼動中いつでも計測情報入力部169より入力し更新することが可能であるとする。

【0041】図2に、本実施例の情報サーバ装置における公開鍵暗号処理の処理手続きの流れを、SSLの通信手順を用いて端末装置500と通信する例で説明する。

【0042】情報サーバ装置の通常OSの暗号化通信によるアクセス処理部163は、セキュアOSの秘密鍵を用いた暗号復号処理部153と暗号情報をやり取りするため、論理分割制御システムの暗号情報通信部141に対して経路確保を要求する(ステップ200)。一方のセキュアOSの暗号復号処理部153も、暗号情報通信部141に対して経路確保を要求する(ステップ220)。この経路確保とは、先に説明したメモリ領域を用いたOS間の通信の場合は、通信に用いるメモリ領域を論理分割制御システムに対しあらかじめ通知する処理等である。

【0043】暗号化通信によるアクセス処理部163は、その後、端末装置500から公開鍵暗号通信開始要求520を受け付ける(ステップ201)。アクセス処理部163は、端末装置500へ公開鍵情報521を送付する(ステップ202)。アクセス処理部163は、端末装置500から暗号化情報522を受け取り(ステップ203)、受信した暗号化情報522を、暗号情報通信部141を介してセキュアOSの復号化処理部153へ送付する(ステップ204)。暗号復号処理部153は、暗号化通信によるアクセス処理部163からの復号依頼を受け付け(ステップ221)、秘密鍵151を使って、暗号化された情報を復号処理(ステップ222)、復号した情報を、暗号情報通信部141を介して通常OSのアクセス処理部163へ送付する(ステップ223)。アクセス処理部163は、復号化された情報を受信し(ステップ205)、復号化した情報から共通鍵に関する情報を取り出す(ステップ206)。前記ステップ206で取り出した共通鍵を用いて、情報サーバ装置から送付する情報を暗号化し、返信する情報523を作成し(ステップ207)、端末装置500へ送付する(ステップ208)。アクセス処理部163は、端末装置500から共通鍵で暗号化された情報524を必要に応じて受け取り(ステップ209)、共通鍵を用いて復号化し、処理する(ステップ210)。そして、前記復号化した情報に応じて、端末装置500へ返信する情報を作成する(ステップ207)。

【0044】図3に、本実施例の情報サーバ装置における資源利用状況の計測処理の流れを示す。情報サーバ装置の通常OSの資源利用状況計測部166は、セキュアOSの資源利用状況計測部154と資源利用状況に関する情報をやり取りするため、論理分割制御システムの資源利用状況通信部142に対して経路確保を要求する(ステップ300)。一方のセキュアOSの資源利用状況計測部154も、資源利用状況通信部142に対して経路確保を要求する(ステップ320)。資源利用状況計測部166は、計測情報入力部169に対し、閾値情報と計測間隔情報の入力依頼をし、システム管理者から情報入力してもらう(ステップ310)。本実施例では、起動時にシステム管理者が閾値情報と計測間隔情報を入力するとしたが、前述のようにこれらの情報をあらかじめ磁気ディスク装置121に格納しておき、資源利用状況計測部166起動時に磁気ディスク装置121内から読み出す方法でもよい。

【0045】前記ステップ310により、閾値情報167には、通常OSのCPU使用率の閾値167-1、通常OSのメモリ使用率の閾値167-2、セキュアOSのCPU使用率の閾値167-3、セキュアOSのメモリ使用率の閾値167-4という、4つの値が格納される。また、計測間隔情報168には、計測間隔の時間情報が格納される。

【0046】資源利用状況計測部166は、計測間隔情報168を参照し、次に計測する時刻を現在の時刻から算出し、その時刻になるまで待つ(ステップ301)。前記待機する手段としては、一般的に、OSが提供しているタイマー機能を利用する。例えば、通常OSに対し、ある一定の間隔で計測情報入力部166の処理を稼動させる、という設定で本発明を実施してもかまわない。

【0047】次に、資源利用状況計測部166は、設定した時刻になると、通常OSでのCPU使用率、および、メモリ使用率を計測し(ステップ302)、セキュアOSにCPU使用率およびメモリ使用率の計測を依頼する(ステップ303)。

【0048】一方、セキュアOSの資源利用状況計測部154は、通常OSとの通信経路確保320の後、通常OSからCPU使用率およびメモリ使用率の計測依頼が来るのを待ち(ステップ321)、計測依頼を受信する(ステップ322)。資源利用状況計測部154は、セキュアOSでのCPU使用率、および、メモリ使用率を計測し(ステップ323)、通常OSへ計測情報を通知し(ステップ324)、次の計測依頼を受信するまで待機する(ステップ321)。

【0049】通常OSの資源利用状況計測部166は、セキュアOSからCPU使用率の情報、および、メモリ使用率の情報を得る(ステップ304)。資源利用状況計測部166は、前記資源利用状況の計測情報、すなわ

ち、通常OSのCPU使用率と、通常OSのメモリ使用率と、セキュアOSのCPU使用率と、セキュアOSのメモリ使用率の情報と、計測した日時とを、磁気ディスク装置121内の資源利用状況計測情報172へ格納する(ステップ305)。

【0050】資源利用状況計測部166は、閾値情報167を参照し、計測した通常OSとセキュアOSそれぞれのCPU使用率とメモリ使用率の情報が、閾値を超えているかどうかを調べる(ステップ306)。

【0051】具体的には、通常OSのCPU使用率と閾値情報167-1、通常OSのメモリ使用率と閾値情報167-2、セキュアOSのCPU使用率と閾値情報167-3、セキュアOSのメモリ使用率と閾値情報167-4とを比較し、計測した使用率の値が閾値を超えたかどうかを確かめる。いずれかの比較においても閾値を超えなかった場合には、ステップ301へ進み、計測間隔情報168を参照して次の計測時刻を算出し、その時刻になるまで待つ。また、いずれかの比較において、閾値を超えたものがあつた場合には、システム管理者に対し、計算機資源の計測結果と、閾値を超えた資源があることを通知する(ステップ307)。前記システム管理者は、端末装置132を使って、本情報サーバ装置の資源利用状況計測部166からの通知を待ちながら、他の仕事をしてもよい。

【0052】次に、システム管理者が、情報サーバ装置に対して通常OSとセキュアOSに資源を配分し、起動できる状態にする、すなわちインストールの手順と、前記、資源利用状況計測部166から何らかの計算機資源が閾値を超えている旨を受信した場合に、計算機の資源を再配分する手順について説明する。再配分の作業は、通知を受けた端末装置132からネットワーク130を介して行っても良いが、ネットワークのセキュリティが低い場合は、好ましくは前述のとおり入力装置110と画面表示装置111を用いて直接情報サーバ装置5に入力する方がよい。

【0053】なお、本実施例の論理分割制御システムには、情報サーバ装置のCPU資源1~4を本情報サーバ装置で稼動させるOSに対し、時分割で共用させる機能を備えているものとする。

【0054】また、本実施例の情報サーバ装置に備える入出力装置にはそれぞれ、割り込み要求(Interrupt Request)番号がわりふられているものとする。前記割り込み要求とは、前記入出力装置が、CPUの処理中に前記入出力装置の処理を割り込ませるためCPUへ送る要求のことであり、割り込み要求番号とは、その要求がどの入出力装置から送付されたものかを識別するために用いる番号である。本実施例では、磁気ディスク装置120の入出力を司るI/Oアダプタ104に、割り込み要求番号「0x0B」を割り当て、磁気ディスク装置121の入出力を司るI/Oアダプタ10

5に、割り込み要求番号「0x0C」を割り当て、磁気ディスク装置122の入出力を司るI/Oアダプタ106に、割り込み要求番号「0x0E」を割り当て、ネットワーク130の入出力を司るネットワーク用アダプタ107に、割り込み要求番号「0x0D」を割り当て、前記割り込み要求番号をシステム管理者が認識しているものとする。

【0055】また、本実施例では、通常OSまたはセキュアOSのインストールを行う際に、まずFDに格納されている起動用プログラムを用いて起動した後に、通常OSまたはセキュアOSのインストール作業を開始するものとする。一般的には、インストールするOSに関する情報は、1枚のフロッピー（登録商標）ディスクに納まらないほど情報量が多いため、CD-ROMを利用または併用し、CD-ROMからOSのインストール先、具体的には、磁気ディスク装置のしかるべき位置へ情報をコピーするのが一般的である。本実施例では、フロッピーディスクとCD-ROMを併用してインストール作業をし、インストール後は、OSを格納した磁気ディスク装置から起動するものとする。

【0056】図5に、論理分割制御システムの論理分割制御部143に対して、入力装置110から、通常OSとセキュアOSの計算機資源について初期設定する際のコマンド入力画面を示す。前記コマンド入力画面に対する操作は、システム管理者が行うものとする。

【0057】まず、論理分割制御部143に対し、「devlist」コマンドを入力し（601）、情報サーバ装置に接続してあるデバイス、すなわち、FDドライブ112と、CD-ROMドライブ113と、磁気ディスク装置120～122の一覧を表示させ、情報サーバ装置に接続しているデバイスを識別するための情報としてそれぞれのデバイスに固有に割り振られた番号を得る。本実施例では、FDドライブ112のデバイス番号は01であり（602）、1台目の磁気ディスク装置のデバイス番号は80であり（603）、2台目の磁気ディスク装置のデバイス番号は81であり（604）、3台目の磁気ディスク装置のデバイス番号は82であり（605）、CD-ROMドライブ113のデバイス番号はFFである（606）。

【0058】次に、論理分割制御部143に対し、通常OS用の計算機資源を設定する（607）。具体的には、「set」コマンドを入力装置110から入力し、そのコマンドの引数として、論理分割単位の名称となる「normal-OS」と（608）、最初のCPU使用比率の割り当てとなる、CPU全体の使用率に対する割合「40」パーセント（%）と（609）、通常OSが使用する物理的なメモリ容量「2048」メガバイト（MB）と（610）、OS起動用のデバイスとしてFDを使うために、そのFDを識別するための情報である、前記手順602で調べたFDドライブのデバイス番

号「01」と（611）、ネットワーク用アダプタ107および磁気ディスク装置121を利用するために、あらかじめ設定しておいた割り込み要求番号「0x0C」と「0x0D」を指定する（612）。論理分割制御部143は、「set」コマンドの要求を受け付け、システム管理者が要求した通常OSに割り当てる計算機資源の確保をする。

【0059】次に、通常OSをインストールする作業をとり行うためのフロッピーディスクをFDドライブ112へ挿入し、各種通常OSに関する情報を格納してあるCD-ROMをCD-ROMドライブ113へ挿入する。

【0060】次に、論理分割制御部143に対し、通常OSの計算機資源を実際に使用可能な状況にするために、「activate」コマンドを入力する（613）。具体的には、「activate」コマンドを入力装置110から入力し、そのコマンドの引数として、通常OSの論理分割単位の名称である「normal-OS」を指定する（614）。論理分割制御部143

は、「activate」コマンドの要求を受け付け、論理的に通常OSを稼働させるために確保した計算機資源を利用可能にし、FDドライブ112からフロッピーディスク内に格納されている起動用プログラムを読み出し、論理的に計算機資源を起動し、OSのインストール作業を開始する。通常OSに関する様々な情報をCD-ROMドライブ113から読み出し、磁気ディスク装置121へ格納する。

【0061】前記通常OSのインストール後、システム管理者は論理分割制御部143に対し、通常OSの起動用デバイスを、FDドライブ112から通常OSをインストールした磁気ディスク装置121にきりかえる（615）。具体的には、「set」コマンドを入力装置110から入力し、そのコマンドの引数として、論理分割単位の名称である「normal-OS」と（616）OS起動用の磁気ディスク装置121のデバイス番号「81」を指定する（617）。

【0062】次に、論理分割制御部143に対し、セキュアOS用の計算機資源を設定する（618）。具体的には、「set」コマンドを入力装置110から入力し、そのコマンドの引数として、論理分割単位の名称となる「secure-OS」と（619）、最初のCPU使用比率の割り当てとなる、CPU全体の使用率に対する割合「60」パーセント（%）と（620）、セキュアOSが使用する物理的なメモリ容量「1024」メガバイト（MB）と（621）、OS起動用のデバイスとしてFDを使うために、前記手順602で調べたFDドライブのデバイス番号「01」と（622）、磁気ディスク装置122を利用するために、あらかじめ設定しておいた割り込み要求番号「0x0E」を指定する（623）。論理分割制御部143は、「set」コマンドの

要求を受け付け、システム管理者が要求したセキュアOSに割り当てる計算機資源の確保をする。

【0063】次に、セキュアOSをインストールする作業をとり行うためのフロッピーディスクをFDドライブ112へ挿入し、各種セキュアOSに関する情報を格納してあるCD-ROMをCD-ROMドライブ113へ挿入する。

【0064】次に、論理分割制御部143に対し、セキュアOSの計算機資源を実際に使用可能な状況にするために、「activate」コマンドを入力する(624)。具体的には、「activate」コマンドを入力装置110から入力し、そのコマンドの引数として、セキュアOSの論理分割単位の名称である「secure-OS」を指定する(625)。論理分割制御部143は、「activate」コマンドの要求を受け付け、論理的にセキュアOSを稼働させるために確保した計算機資源を利用可能にし、FDドライブ112からフロッピーディスク内に格納されている起動用プログラムを読み出し、論理的に計算機資源を起動し、OSのインストール作業を開始する。セキュアOSに関する様々な情報をCD-ROMドライブ113から読み出し、磁気ディスク装置122へ格納する。

【0065】前記セキュアOSのインストール後、システム管理者は論理分割制御部143に対し、セキュアOSの起動用デバイスを、FDドライブ112からセキュアOSをインストールした磁気ディスク装置122にきりかえる(626)。具体的には、「set」コマンドを入力装置110から入力し、そのコマンドの引数として、論理分割単位の名称である「secure-OS」と(627)OS起動用の磁気ディスク装置122のデバイス番号「82」を指定する(628)。

【0066】以上のコマンド入力手続き601~628*

$$60(\%) \times 0.9 = 54(\%) \cdots \cdots \text{セキュアOSのCPU使用比率}$$

と算出する。

【0072】ステップ403で算出した新たなセキュアOSのCPU使用比率から、通常OSのCPU使用比率※

$$100(\%) - 54(\%) = 46(\%) \cdots \cdots \text{通常OSのCPU使用比率}$$

と算出する。その後、ステップ407へ進む。

【0073】一方、CPUの使用率が閾値を超えたのがセキュアOSだった場合、通常OSの現状のCPU使用比率(本実施例では40%)をある一定の割合で減らし

$$40(\%) \times 0.9 = 36(\%) \cdots \cdots \text{通常OSのCPU使用比率}$$

$$100(\%) - 36(\%) = 64(\%) \cdots \cdots \text{セキュアOSのCPU使用比率}$$

と算出する。

【0074】前記ステップ403~406で算出した新たなCPU使用比率を、入力装置110から、論理分割制御部143に対して設定する(ステップ407)。設定後、ステップ410へ進む。

【0075】次に、システム管理者が資源利用状況計測部166から受信した情報を再度参照し、メモリの使用

*により、通常OSとセキュアOSがインストールされ、各OSの制御の元で、前記暗号化通信によるアクセス処理部163や、資源利用状況計測部166や、秘密鍵を用いた暗号復号処理部153や、資源利用状況計測部154が稼働する。

【0067】次に、システム管理者が、前記資源利用状況計測部166から何らかの計算機資源が閾値を超えている旨を受信した場合に、計算機資源を再配分する処理手順を図4、図6を用いて説明する。

【0068】図4に、システム管理者が資源利用状況計測部166から受信した情報をもとに、新たなCPU使用比率またはメモリ容量を具体的に決定し、再設定する手順を示す。

【0069】システム管理者が資源利用状況計測部166から受信した情報を参照し、CPUの使用率が閾値を超えていたという通知かどうかを判断する(ステップ401)。CPUの使用率が閾値を超えていた場合には、手続き402へ進み、超えていなかった場合は、手続き410へ進む。

【0070】CPUの使用率が閾値を超えていた場合には、閾値を超えたのは通常OSなのか、セキュアOSなのか、その両方のOSなのかを判断する(ステップ402)。通常OSだった場合には、手続き403へ進み、セキュアOSだった場合には、手続き405へ進み、両方のOSだった場合には、情報サーバ装置のCPU資源全体が足りないということになるため、現状のCPU使用比率の設定は変更せず、手続き410へ進む。

【0071】CPUの使用率が閾値を超えたのが通常OSだった場合、セキュアOSの現状のCPU使用比率(本実施例では60%)をある一定の割合で減らす(ステップ403)。例えば、現使用比率の1割を減らす場合には、

$$60(\%) \times 0.9 = 54(\%) \cdots \cdots \text{セキュアOSのCPU使用比率}$$

※を算出する(ステップ404)。前記の例を引き続き用いると、

★(ステップ405)、新たな通常OSのCPU使用比率から、セキュアOSのCPU使用比率を算出する(ステップ406)。例えば、現使用比率の1割を減らす場合には、

率が閾値を超えていたという通知かどうかを判断する(ステップ410)。メモリの使用率が閾値を超えていた場合には、手続き411へ進み、超えていなかった場合は、本再設定の処理を終了する(ステップ420)。

【0076】メモリの使用率が閾値を超えていた場合には、本情報サーバ装置に未使用のメモリ資源が残されているかどうかを確認し(ステップ411)、もし残って

いれば、未使用のメモリ資源の一部または全部を、閾値を超えてしまったOSのメモリ資源として割り当てる(ステップ412)。割り当てる量については、CPU使用率を算出したときのように一定の割合量を増やしてもよいし、必要と思われる量を増やしてもよい。例えば、セキュアOSのメモリ容量、1024MBが足りなくなり、2048MBの未使用のメモリ資源があった場合、セキュアOSに対し2倍のメモリ容量となる2048MBのメモリ資源を割り当てる、といった手順で算出する。その後、ステップ418へ進む。

【0077】ステップ411で、本情報サーバ装置に未使用のメモリ資源が残されていないと判断した場合、メモリ使用率の閾値を超えたのは通常OSなのか、セキュアOSなのか、その両方のOSなのかを判断する(ステ*

$$\begin{aligned} & 1024 \text{ (MB)} \times 0.75 = 768 \text{ (MB)} \cdots \text{セキュアOSのメモリ容量} \\ & 2048 \text{ (MB)} + (1024 \text{ (MB)} - 768 \text{ (MB)}) \\ & = 2304 \text{ (MB)} \cdots \text{通常OSのメモリ容量} \end{aligned}$$

と算出する。その後、ステップ418へ進む。

【0079】一方、メモリ使用率が閾値を超えたのがセキュアOSだった場合、通常OSの現状のメモリ容量(本実施例では2048MB)をある一定の割合で減らし(※

$$\begin{aligned} & 2048 \text{ (MB)} \times 0.75 = 1536 \text{ (MB)} \cdots \text{通常OSのメモリ容量} \\ & 1024 \text{ (MB)} + (2048 \text{ (MB)} - 1536 \text{ (MB)}) \\ & = 1536 \text{ (MB)} \cdots \text{セキュアOSのメモリ容量} \end{aligned}$$

と算出する。

【0080】前記ステップ414～417で算出した新たなメモリ容量を、入力装置110から、論理分割制御部143に対して設定し(ステップ418)、本再設定の処理を終了する(ステップ420)。

【0081】図6に、前記ステップ407およびステップ411およびステップ418で、本情報サーバ装置の計算機資源を再設定したり、未使用のメモリ資源を確認する際の、コマンド入力画面を示す。前記コマンド入力画面に対して行う操作は、入力装置110を介して論理分割制御システムの論理分割制御部143に伝わるものとする。また、以下の実施例では、すでに通常OSとセキュアOS用の計算機資源を、手順607と、手順615と、手順618と、手順626で設定してある場合を例にして説明する。

【0082】まず、論理分割制御部143に対して、「lparstat」コマンドを入力し(700)、現状の情報サーバ装置の資源の論理的分割状況と、未使用のメモリ容量の一覧を画面表示装置111に表示させる。

【0083】各論理分割単位を識別するための情報であり、第一の論理分割単位であることを示すラベル「LP1」と(701)、第一の論理分割単位の名称である「normal-OS」と(702)、第一の論理分割単位のCPU使用比率である「40」(%)と(703)、第一の論理分割単位のメモリ容量である「204

* ップ413)。通常OSだった場合には、手続き414へ進み、セキュアOSだった場合には、手続き416へ進み、両方のOSだった場合には、情報サーバ装置のメモリ資源全体が足りないということになるため、現状のメモリ容量の設定は変更せず、本再設定の処理を終了する(ステップ420)。

【0078】メモリの使用率が閾値を超えたのが通常OSだった場合、セキュアOSの現状のメモリ容量(本実施例では1024MB)をある一定の割合で減らし(ステップ414)、前記減らしたメモリ容量を、通常OSに新たに割り当てる(ステップ415)。例えば、セキュアOSの使用量の2.5割を通常OSに割り当てる場合には、

※ステップ416)、前記減らしたメモリ容量を、セキュアOSに新たに割り当てる(ステップ417)。例えば、通常OSの使用量の2.5割をセキュアOSに割り当てる場合には、

2048 (MB) × 0.75 = 1536 (MB) … 通常OSのメモリ容量
1024 (MB) + (2048 (MB) - 1536 (MB)) = 1536 (MB) … セキュアOSのメモリ容量
8」(MB)と(704)、第一の論理分割単位で使用するOS起動用のデバイスの番号である「81」と(705)、第一の論理分割単位で使用する割り込み要求番号である「0x0C 0x0D」(706)を表示する。

【0084】引き続き、第二の論理分割単位であることを示すラベル「LP2」と(710)、第二の論理分割単位の名称である「secure-OS」と(711)、第二の論理分割単位のCPU使用比率である「60」(%)と(712)、第二の論理分割単位のメモリ容量である「1048」(MB)と(713)、第二の論理分割単位で使用するOS起動用のデバイスの番号である「82」と(714)、第二の論理分割単位で使用する割り込み要求番号である「0x0E」(715)を表示する。

【0085】引き続き、未使用のメモリ容量を表示するためのラベル「Memory distribution」と(720)、通常OSに割り当てられているメモリ容量を示す「LP1 normal-OS 2048 (MB)」(721)と、セキュアOSに割り当てられているメモリ容量を示す「LP2 secure-OS 1024 (MB)」(722)と、未使用のメモリ容量を示す「Remaining RAM 0 (MB)」(723)を表示する。本実施例では、未使用のメモリがない、すなわち、情報サーバ装置に備えるすべてのメモリ資源を、通常OSまたはセキュアOSへ割り当てて

いるものとする。未使用のメモリ資源がある場合には、未使用のメモリ容量「Remaining RAM」欄に未使用のメモリ容量の値が表示される。

【0086】次に、「lparstat」コマンドで情報を表示させた後、CPU使用比率と、メモリ容量を設定する手順を示す。本実施例では、通常OSのCPU使用率と通常OSのメモリ使用率とが閾値を超え、セキュアOSのCPU使用率の1割分と、セキュアOSのメモリ容量の2.5割分を通常OSの計算機資源として再設定する例を示す。

【0087】まず、論理分割制御部143に対して、「set」コマンドを用いて、通常OSの計算機資源の情報を更新する(730)。コマンドの引数として、論理分割単位の名称である「normal-OS」と(731)と、CPU使用比率「46」(%)と(732)、メモリ容量「2304」(MB)を指定する(733)。

【0088】引き続き、論理分割制御部143に対して、「set」コマンドを用いて、セキュアOSの計算機資源の情報を更新する(740)。コマンドの引数として、論理分割単位の名称である「secure-OS」と(741)と、CPU使用比率「54」(%)と(742)、メモリ容量「768」(MB)を指定する(743)。

【0089】本実施例では手順730および手順740の操作を、通常OSおよびセキュアOSが稼動している最中でも指定可能である論理分割制御システムを前提にしている。前記再設定の操作のために、稼動中のOSを一度停止させなければならない論理分割制御システムの場合には、以下に示す手順となる。

【0090】手順730を実施する前に、通常OSにて、通常OSを停止させる「シャットダウン」操作を行う。次に、論理分割制御部143に対し、通常OSの計算機資源を使用不可能な状況にするために、「deactivate」コマンドを入力し、そのコマンドの引数として、通常OSの論理分割単位の名称である「normal-OS」を指定する。次に手順730を実施し、通常OSの計算機資源を使用可能な状況にするために、「activate」コマンドを入力し、そのコマンドの引数として、通常OSの論理分割単位の名称である「normal-OS」を指定する。

【0091】同様に、手順740を実施する前に、セキュアOSにて、セキュアOSを停止させる「シャットダウン」操作を行う。次に、論理分割制御部143に対し、セキュアOSの計算機資源を使用不可能な状況にするために、「deactivate」コマンドを入力し、そのコマンドの引数として、セキュアOSの論理分割単位の名称である「secure-OS」を指定する。次に手順740を実施し、セキュアOSの計算機資源を使用可能な状況にするために、「activate」コ

マンドを入力し、そのコマンドの引数として、セキュアOSの論理分割単位の名称である「secure-OS」を指定する。

【0092】なお、本実施例では、情報サーバ装置で稼動させるOSとして、端末装置との情報通信全般を司る通常OSと、暗号処理を司るセキュアOSを稼動させる例を述べたが、セキュアOSの変わりに、別の処理を専門とするOSを稼動させても構わない。

【0093】例えば、従来のWebサーバシステムでは、データベースへのアクセスを受け付け、Webサーバに接続するデータベースの内容に応じて、端末装置へ送付する表示内容を動的に生成する機能を備えているものもある。当該Webサーバでは、端末装置からの要求をデータベースに伝えるために、CGI(Common Gateway Interface)というインターフェースを用いるが、CGIを処理するプログラムがWebサーバのCPU負荷をかける原因となることが判っている。そこで、CGI用のOSを稼動し、CGI用OSに対し計算機資源を割り当て、通常OSからCGI用OSへCGIの処理を依頼する。このことで、CGIの処理により発生していたWebサーバの反応速度の低下を回避することが可能となる。

【0094】

【発明の効果】本発明によれば、特別なアクセラレータ装置を装備しない情報サーバ装置において、少なくとも非暗号通信のアクセスに対する反応速度低下を回避することが可能となり、さらには、秘密鍵の漏洩防止が可能となる。

【図面の簡単な説明】

【図1】情報サーバ装置の構成図

【図2】情報サーバ装置における暗号処理の流れ

【図3】資源利用状況計測部の処理の流れ

【図4】CPU使用比率とメモリ容量の決定および設定手続きの流れ

【図5】通常OSとセキュアOSインストール時の計算機資源配分のコマンド入力画面

【図6】通常OSとセキュアOSの計算機資源再配分のコマンド入力画面

【符号の説明】

1〜4…情報サーバ装置に備えるCPU

5…情報サーバ装置に備えるメモリ

110…情報サーバ装置に備える入力装置

111…情報サーバ装置に備える画面表示装置

112…情報サーバ装置に備えるFDドライブ

113…情報サーバ装置に備えるCD-ROMドライブ

120…論理分割制御システム用磁気ディスク装置

121…通常OS用磁気ディスク装置

122…セキュアOS用磁気ディスク装置

130…ネットワーク

131…公衆網

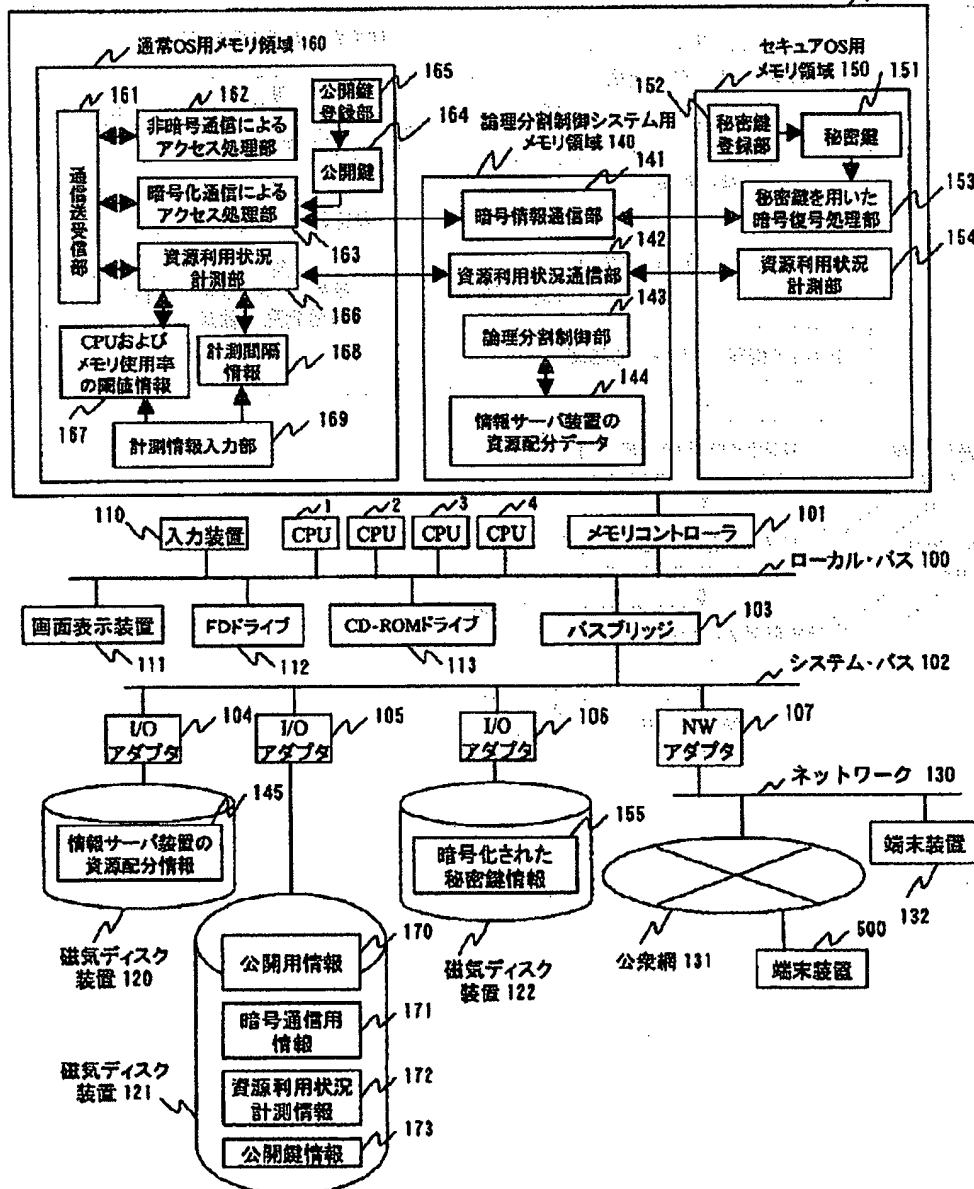
132…システム管理者が閾値を超えた旨を受信する端末装置
 140…論理分割制御システム用メモリ領域
 141…暗号情報通信部
 142…資源利用状況通信部
 143…論理分割制御部
 150…セキュアOS用メモリ領域
 151…秘密鍵
 152…秘密鍵登録部
 153…秘密鍵を用いた暗号復号処理部
 154…秘密鍵を用いた暗号復号処理部

*154…セキュアOSの資源利用状況計測部
 160…通常OS用メモリ領域
 161…通信送受信部
 162…非暗号通信によるアクセス処理部
 163…暗号通信によるアクセス処理部
 164…公開鍵
 165…公開鍵登録部
 166…通常OSの資源利用状況計測部
 500…情報サーバ装置にアクセスする端末装置

*10

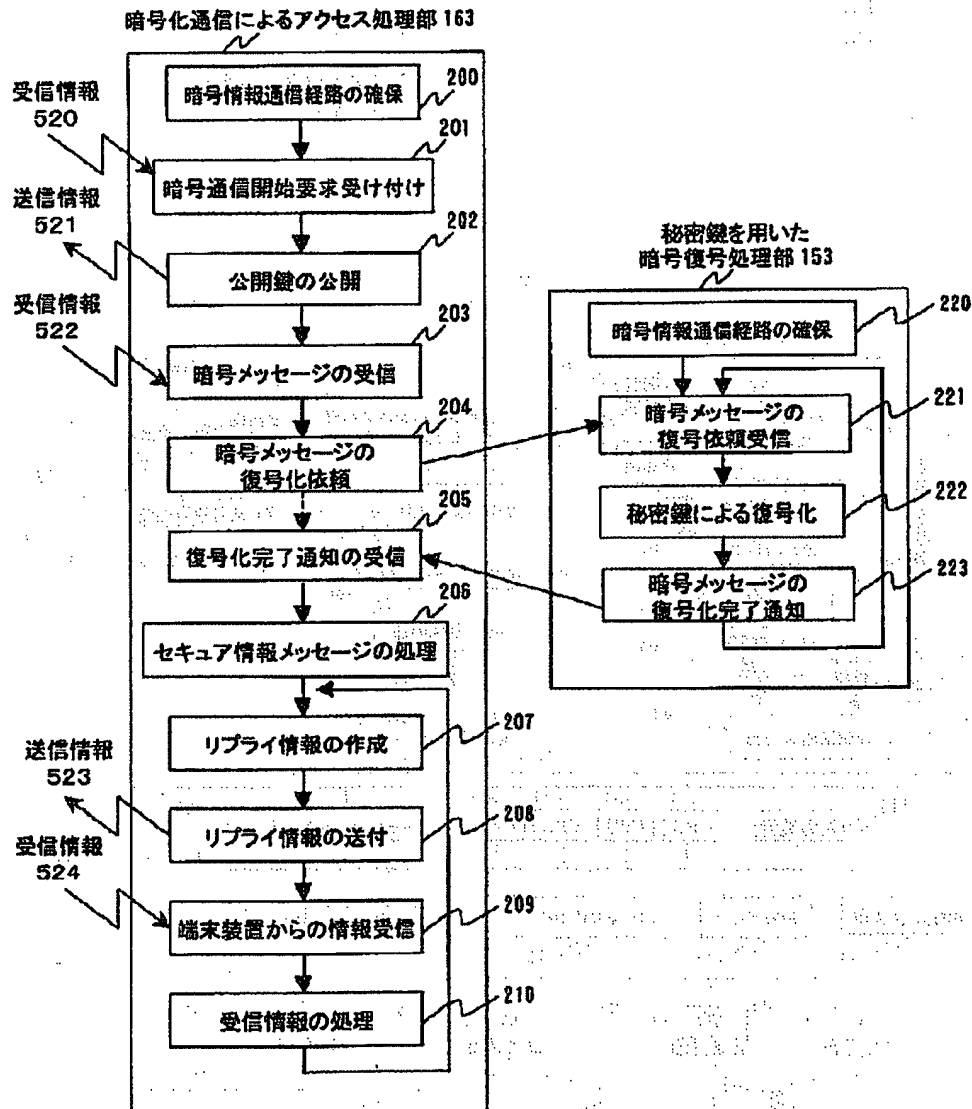
【図1】

図1

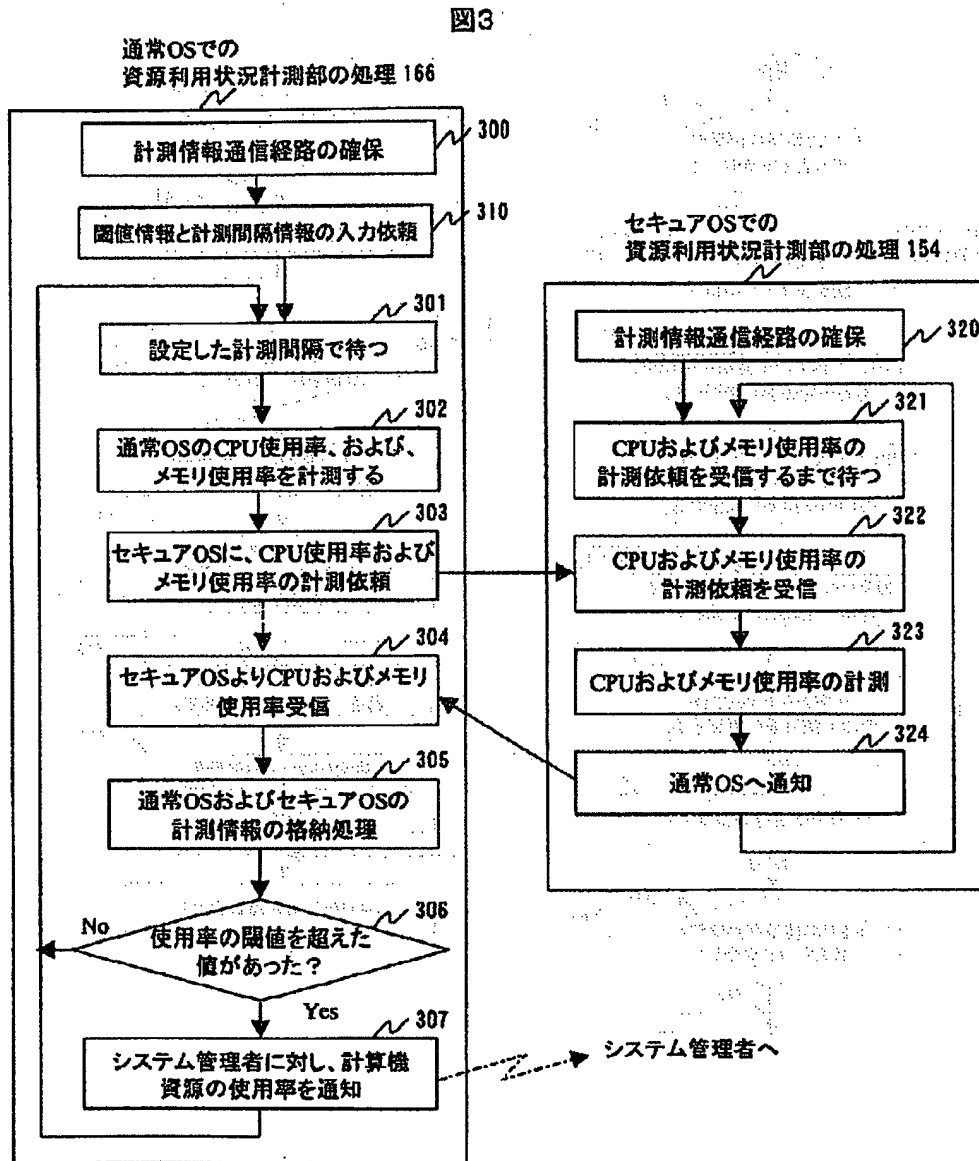


【図2】

図2

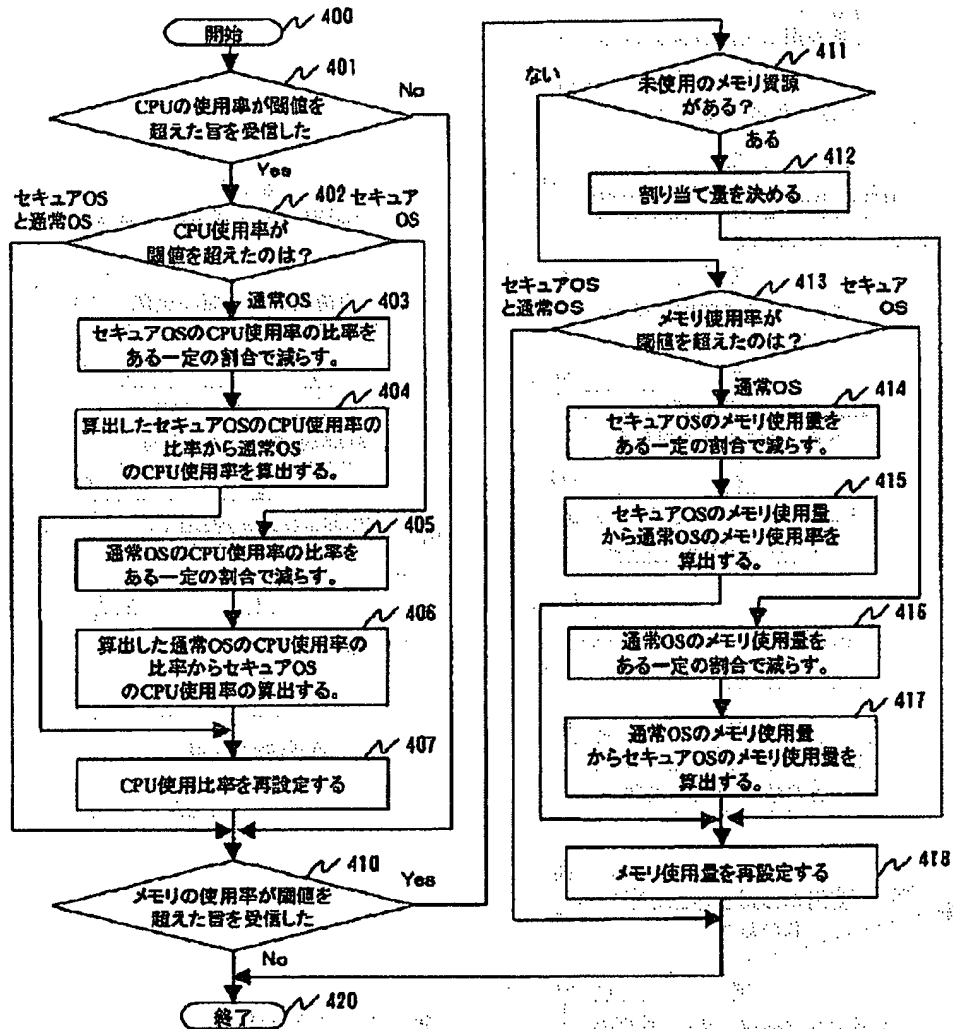


【図3】



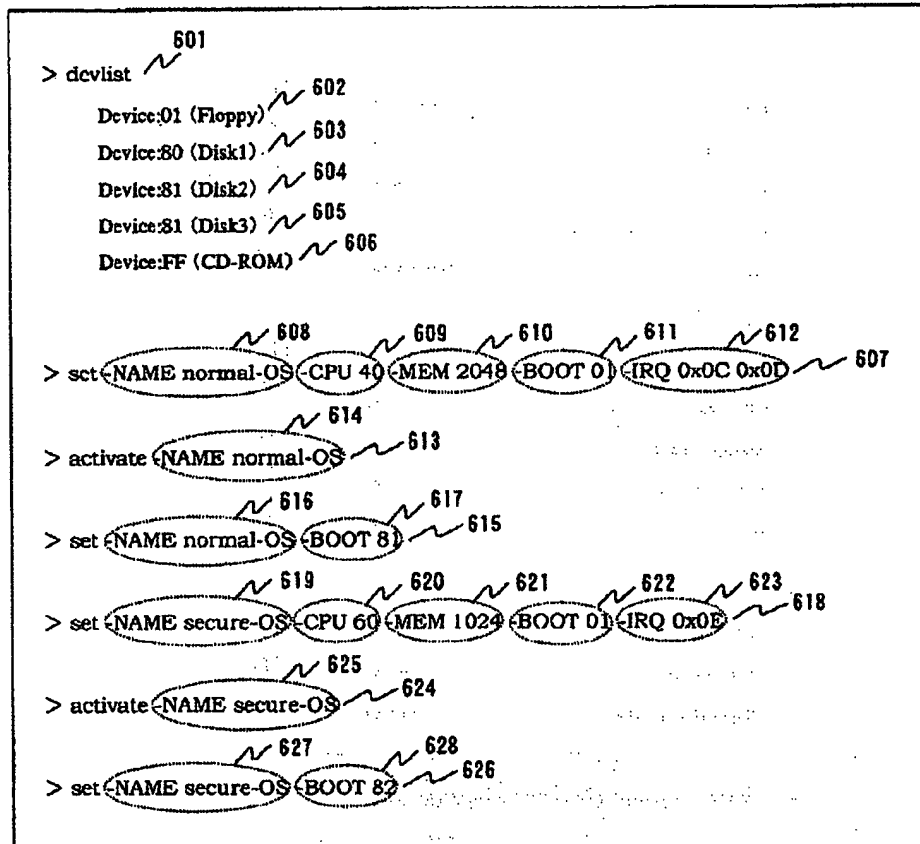
【図4】

図4



【図5】

図5



【図6】

図6

```

> lparstat 700
LP1 701
  LPAR Name      normal-OS 702
  CPU (%)        40 703
  Memory (MB)    2048 704
  BOOT device (Device No.) 81 705
  IRQ            0x0C0x0D 706

LP2 710
  LPAR Name      secure-OS 711
  CPU (%)        60 712
  Memory (MB)    1024 713
  BOOT device (Device No.) 82 714
  IRQ            0x0E 715

Memory distribution 720
  LP1 normal-OS  2048 MB 721
  LP2 secure-OS  1024 MB 722
  Remaining RAM  512 MB 723

> set (NAME normal-OS CPU 46 MEM 2304) 730
    731      732      733
> set (NAME secure-OS CPU 54 MEM 768) 740
    741      742      743

```

フロントページの続き

F ターム(参考) 5B085 AE29 BG07
 5B098 AA10 GC10 GD02 GD03
 5J104 AA01 AA16 AA17 EA04 EA19
 PA07